

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-099187

(43)Date of publication of application : 07.04.2000

(51)Int.Cl.

G06F 1/00
H04B 7/26
H04L 9/32

(21)Application number : 10-288916

(71)Applicant : SANYO ELECTRIC CO LTD

(22)Date of filing : 24.09.1998

(72)Inventor : KUWATA KAIHEI
KURITA MAKOTO

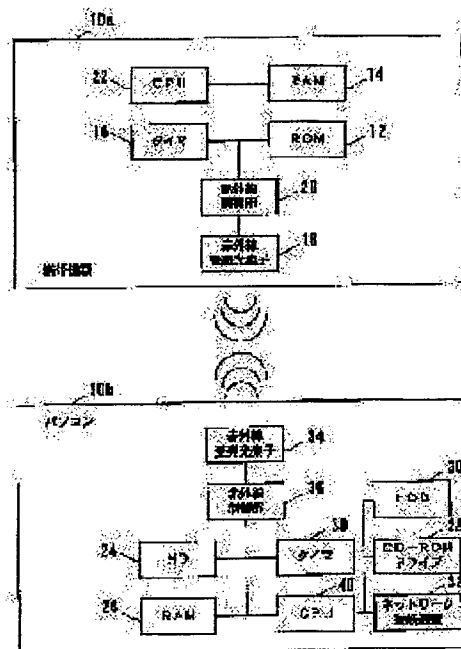
(54) SYSTEM AND METHOD FOR RADIO COMMUNICATIONS, AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To sufficiently protect the privacy of user information by identifying a user without complicated operation.

SOLUTION: User identification information is cyclically transmitted from a portable equipment 10a to a personal computer(PC) 10b.

Corresponding to that transmission, the PC 10b judges whether the received user identification information is coincident with identification information registered in a RAM 26 or not, and when the information is mutually coincident, the utilization of the PC is permitted to that user but when the information is not coincident, the utilization of the PC is not permitted to that user. This processing is periodically performed. Besides, the user identification information can be changed by the PC 10b as well. Further, the password of a file prepared by the PC 10b is updated into password transmitted from the portable equipment 10a and the file can be managed as well.



LEGAL STATUS

[Date of request for examination] 28.06.2002

[Date of sending the examiner's decision of rejection] 01.02.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-99187

(P2000-99187A)

(43) 公開日 平成12年4月7日(2000.4.7)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 1/00	3 7 0	G 0 6 F 1/00	3 7 0 E 5 J 1 0 4
H 0 4 B 7/26		H 0 4 B 7/26	E 5 K 0 6 7
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A

審査請求 未請求 請求項の数17 F D (全 11 頁)

(21) 出願番号 特願平10-288916

(22) 出願日 平成10年9月24日(1998.9.24)

(71) 出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72) 発明者 鉢田 海平

大阪府守口市京阪本通2丁目5番5号 三
洋電機株式会社内

(72) 発明者 栗田 誠

大阪府守口市京阪本通2丁目5番5号 三
洋電機株式会社内

(74) 代理人 100101351

弁理士 辰巳 忠宏

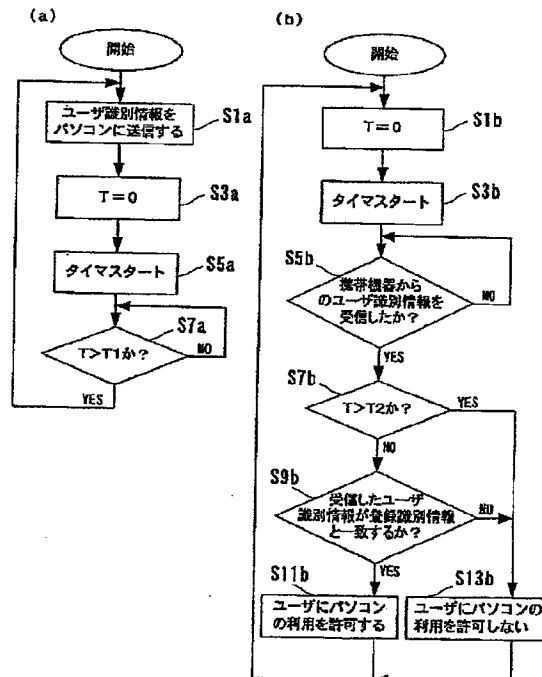
最終頁に続く

(54) 【発明の名称】 無線通信システム、無線通信方法および記録媒体

(57) 【要約】

【課題】 煩雑な操作なしにユーザを識別しユーザ情報の秘匿性を十分に保護する。

【解決手段】 携帯機器10aからパソコン10bへ周期的にユーザ識別情報を送信する。それに応じてパソコン10bでは、受信したユーザ識別情報とRAM26に登録されている識別情報とが一致するか否かを判断し、一致すればそのユーザにパソコンの利用を許可し、一致しなければそのユーザにパソコンの利用を許可しない。この処理を周期的に行う。また、パソコン10bによってユーザ識別情報を変更してもよい。さらに、パソコン10bで作成したファイルのパスワードを、携帯機器10aから送信されたパスワードに更新し、ファイルを管理してもよい。



【特許請求の範囲】

【請求項 1】 ユーザが携帯可能でありかつ無線通信可能な第 1 装置と無線通信可能な第 2 装置とを含む無線通信システムであって、

前記第 1 装置はユーザごとの固有のユーザ識別情報を前記第 2 装置に送信する第 1 送信手段を含み、

前記第 2 装置は、前記第 1 装置からの前記ユーザ識別情報を受信する第 2 受信手段、受信した前記ユーザ識別情報に基づいてユーザを識別する識別手段、および前記識別手段によるユーザ識別結果に従って前記ユーザに利用許可を与える許可手段を含む、無線通信システム。

【請求項 2】 前記第 2 装置は、前記第 2 受信手段によって受信した前記ユーザ識別情報を変更する第 2 変更手段、および前記第 1 装置に変更後のユーザ識別情報を送信する第 2 送信手段をさらに含み、

前記第 1 装置は、前記第 2 装置から送信された前記変更後のユーザ識別情報を受信する第 1 受信手段、および前記第 1 送信手段から送信するユーザ識別情報を前記変更後のユーザ識別情報に更新する第 1 更新手段をさらに含む、請求項 1 に記載の無線通信システム。

【請求項 3】 ユーザが携帯可能でありかつ無線通信可能な第 1 装置と無線通信可能な第 2 装置とを含む無線通信システムであって、

前記第 1 装置は、ユーザごとの固有のユーザ識別情報を前記第 2 装置に送信する第 1 送信手段、前記第 2 装置から送信された変更後のユーザ識別情報を受信する第 1 受信手段、および前記第 1 送信手段から送信するユーザ識別情報を前記変更後のユーザ識別情報に更新する第 1 更新手段を含み、

前記第 2 装置は、前記第 1 装置からの前記ユーザ識別情報を受信する第 2 受信手段、受信した前記ユーザ識別情報を変更する第 2 変更手段、および前記第 1 装置に前記変更後のユーザ識別情報を送信する第 2 送信手段を含む、無線通信システム。

【請求項 4】 前記ユーザ識別情報はユーザ ID とパスワードとを含み、

前記第 2 装置は、前記ユーザ ID と前記パスワードとに基づいてファイルを管理する管理手段、および前記第 1 装置からのユーザ ID に基づいて特定されるファイルのパスワードを更新する第 2 更新手段をさらに含む、請求項 2 または 3 に記載の無線通信システム。

【請求項 5】 前記第 1 装置の前記第 1 送信手段からは前記ユーザ識別情報が周期的に送信される、請求項 1 ないし 4 のいずれかに記載の無線通信システム。

【請求項 6】 前記第 1 装置と前記第 2 装置とは赤外線によって通信される、請求項 1 ないし 5 のいずれかに記載の無線通信システム。

【請求項 7】 前記第 1 装置は携帯機器を含み、前記第 2 装置はパソコンを含む、請求項 1 ないし 6 のいずれかに記載の無線通信システム。

【請求項 8】 ユーザが携帯可能でありかつ無線通信可能な第 1 装置と無線通信可能な第 2 装置との無線通信方法であって、

前記第 1 装置からユーザごとの固有のユーザ識別情報を前記第 2 装置に送信するステップ、

前記第 1 装置からの前記ユーザ識別情報を前記第 2 装置が受信するステップ、

前記第 2 装置が受信した前記ユーザ識別情報に基づいてユーザを識別するステップ、およびユーザ識別結果に従って前記ユーザに利用許可を与えるステップを備える、無線通信方法。

【請求項 9】 前記第 2 装置が受信した前記ユーザ識別情報を変更するステップ、

前記第 2 装置から前記第 1 装置に変更後のユーザ識別情報を送信するステップ、

前記第 2 装置から送信された前記変更後のユーザ識別情報を前記第 1 装置が受信するステップ、および前記第 1 装置から送信するユーザ識別情報を前記変更後のユーザ識別情報に更新するステップをさらに含む、請求項 8 に記載の無線通信方法。

【請求項 10】 ユーザが携帯可能でありかつ無線通信可能な第 1 装置と無線通信可能な第 2 装置との無線通信方法であって、

前記第 1 装置からユーザごとの固有のユーザ識別情報を前記第 2 装置に送信するステップ、

前記第 1 装置からの前記ユーザ識別情報を前記第 2 装置が受信するステップ、

前記第 2 装置が受信した前記ユーザ識別情報を変更するステップ、

前記第 2 装置から前記第 1 装置に変更後のユーザ識別情報を送信するステップ、

前記第 2 装置から送信された前記変更後のユーザ識別情報を前記第 1 装置が受信するステップ、および前記第 1 装置から送信するユーザ識別情報を前記変更後のユーザ識別情報に更新するステップを備える、無線通信方法。

【請求項 11】 前記ユーザ識別情報はユーザ ID とパスワードとを含み、かつ前記第 2 装置は前記ユーザ ID と前記パスワードとに基づいてファイルが管理可能に構成されるときに用いられる無線通信方法であって、

前記第 1 装置からのユーザ ID に基づいて特定されるファイルのパスワードを更新するステップをさらに含む、請求項 9 または 10 に記載の無線通信方法。

【請求項 12】 前記第 1 装置からは前記ユーザ識別情報が周期的に送信される、請求項 8 ないし 11 のいずれかに記載の無線通信方法。

【請求項 13】 ユーザが携帯可能でありかつ無線通信可能な第 1 装置と無線通信可能な第 2 装置との無線通信を行うためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記第 1 装置からユーザごとの固有のユーザ識別情報を

前記第 2 装置に送信させる処理、
前記第 1 装置からの前記ユーザ識別情報を前記第 2 装置に受信させる処理、
前記第 2 装置が受信した前記ユーザ識別情報に基づいてユーザを識別させる処理、およびユーザ識別結果に従って前記ユーザに利用許可を与えさせる処理をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 14】 前記第 2 装置が受信した前記ユーザ識別情報を変更させる処理、
前記第 2 装置から前記第 1 装置に変更後のユーザ識別情報を送信させる処理、
前記第 2 装置から送信された前記変更後のユーザ識別情報を前記第 1 装置に受信させる処理、および前記第 1 装置から送信するユーザ識別情報を前記変更後のユーザ識別情報に更新させる処理をコンピュータに実行させるためのプログラムをさらに記録した、請求項 13 に記載のコンピュータ読み取り可能な記録媒体。

【請求項 15】 ユーザが携帯可能でありかつ無線通信可能な第 1 装置と無線通信可能な第 2 装置との無線通信を行うためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、
前記第 1 装置からユーザごとの固有のユーザ識別情報を前記第 2 装置に送信させる処理、
前記第 1 装置からの前記ユーザ識別情報を前記第 2 装置に受信させる処理、
前記第 2 装置が受信した前記ユーザ識別情報を変更させる処理、
前記第 2 装置から前記第 1 装置に変更後のユーザ識別情報を送信させる処理、
前記第 2 装置から送信された前記変更後のユーザ識別情報を前記第 1 装置に受信させる処理、および前記第 1 装置から送信するユーザ識別情報を前記変更後のユーザ識別情報に更新させる処理をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 16】 前記ユーザ識別情報はユーザ ID とパスワードとを含み、かつ前記第 2 装置は前記ユーザ ID と前記パスワードとに基づいてファイルが管理可能に構成されるときに用いられるコンピュータ読み取り可能な記録媒体であって、
前記第 1 装置からのユーザ ID に基づいて特定されるファイルのパスワードを更新させる処理をコンピュータに実行させるためのプログラムをさらに記録した、請求項 14 または 15 に記載のコンピュータ読み取り可能な記録媒体。

【請求項 17】 前記第 1 装置から前記ユーザ識別情報を周期的に送信させる処理をコンピュータに実行させるためのプログラムをさらに記録した、請求項 13 ないし 16 のいずれかに記載のコンピュータ読み取り可能な記

録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は無線通信システム、無線通信方法および記録媒体に関し、特にたとえばパソコンのユーザ識別に適用される、無線通信システム、無線通信方法および記録媒体に関する。

【0002】

【従来の技術】 従来、パソコンを特定のユーザにのみ利用させるために様々なユーザ識別手段が用いられている。

【0003】 たとえば、パソコンの起動時にはパスワードなどのユーザ識別情報を入力することでパソコン側でユーザの識別が行われ、利用を許可しているユーザであると判断されればパソコンが起動する。パソコンの起動後は、ユーザが一定時間パソコンにキー入力しなければスクリーンセーバが起動するが、そのスクリーンセーバを解除するにはパスワード等のユーザ識別情報をキー入力することが要求され、入力されたユーザ識別情報に基づいてユーザの識別が行われるものがある。

【0004】 また、同じパスワードを長期間利用することはセキュリティの観点から望ましくないため、ユーザが定期的にパスワードを変更することが奨励されている。また、パソコンで作成したファイルを保存管理する際には、ユーザがファイル毎にファイルの利用権や所有権を設定する方法も用いられる。

【0005】

【発明が解決しようとする課題】 しかし、上述の従来技術では、いずれもユーザが能動的かつ積極的にユーザ識別情報を入力・変更しなければならず、操作が煩雑であった。

【0006】 また、一旦パソコンが起動すれば一定時間内（スクリーンセーバが起動するまで）であれば、パソコンの利用を許可されたユーザがパソコンから離れると他人がそのパソコンを利用することができ、また、その際特定のファイルが開いていれば、そのファイルを他人が利用することが可能となる。したがって従来のユーザ識別手段ではユーザ情報の秘匿性を十分に保護することができなかった。

【0007】 それゆえに、この発明の主たる目的は、煩雑な操作なしにユーザを識別できユーザ情報の秘匿性を十分に保護できる、無線通信システム、無線通信方法および記録媒体を提供することである。

【0008】

【課題を解決するための手段】 上記目的を達成するために、請求項 1 に記載の無線通信システムは、ユーザが携帯可能でありかつ無線通信可能な第 1 装置と無線通信可能な第 2 装置とを含む無線通信システムであって、第 1 装置はユーザごとの固有のユーザ識別情報を第 2 装置に送信する第 1 送信手段を含み、第 2 装置は、第 1 装置か

らのユーザ識別情報を受信する第2受信手段、受信したユーザ識別情報に基づいてユーザを識別する識別手段、および識別手段によるユーザ識別結果に従ってユーザに利用許可を与える許可手段を含むものである。

【0009】請求項2に記載の無線通信システムは、請求項1に記載の無線通信システムにおいて、第2装置は、第2受信手段によって受信したユーザ識別情報を変更する第2変更手段、および第1装置に変更後のユーザ識別情報を送信する第2送信手段をさらに含み、第1装置は、第2装置から送信された変更後のユーザ識別情報を受信する第1受信手段、および第1送信手段から送信するユーザ識別情報を変更後のユーザ識別情報に更新する第1更新手段をさらに含むものである。

【0010】請求項3に記載の無線通信システムは、ユーザが携帯可能でありかつ無線通信可能な第1装置と無線通信可能な第2装置とを含む無線通信システムであって、第1装置は、ユーザごとの固有のユーザ識別情報を第2装置に送信する第1送信手段、第2装置から送信された変更後のユーザ識別情報を受信する第1受信手段、および第1送信手段から送信するユーザ識別情報を変更後のユーザ識別情報に更新する第1更新手段を含み、第2装置は、第1装置からのユーザ識別情報を受信する第2受信手段、受信したユーザ識別情報を変更する第2変更手段、および第1装置に変更後のユーザ識別情報を送信する第2送信手段を含むものである。

【0011】請求項4に記載の無線通信システムは、請求項2または3に記載の無線通信システムにおいて、ユーザ識別情報はユーザIDとパスワードとを含み、第2装置は、ユーザIDとパスワードとに基づいてファイルを管理する管理手段、および第1装置からのユーザIDに基づいて特定されるファイルのパスワードを更新する第2更新手段をさらに含むものである。

【0012】請求項5に記載の無線通信システムは、請求項1ないし4のいずれかに記載の無線通信システムにおいて、第1装置の第1送信手段からはユーザ識別情報が周期的に送信されるものである。

【0013】請求項6に記載の無線通信システムは、請求項1ないし5のいずれかに記載の無線通信システムにおいて、第1装置と第2装置とは赤外線によって通信されるものである。

【0014】請求項7に記載の無線通信システムは、請求項1ないし6のいずれかに記載の無線通信システムにおいて、第1装置は携帯機器を含み、第2装置はパソコンを含むものである。

【0015】請求項8に記載の無線通信方法は、ユーザが携帯可能でありかつ無線通信可能な第1装置と無線通信可能な第2装置との無線通信方法であって、第1装置からユーザごとの固有のユーザ識別情報を第2装置に送信するステップ、第1装置からのユーザ識別情報を第2装置が受信するステップ、第2装置が受信したユーザ識

別情報に基づいてユーザを識別するステップ、およびユーザ識別結果に従ってユーザに利用許可を与えるステップを備える。

【0016】請求項9に記載の無線通信方法は、請求項8に記載の無線通信方法において、第2装置が受信したユーザ識別情報を変更するステップ、第2装置から第1装置に変更後のユーザ識別情報を送信するステップ、第2装置から送信された変更後のユーザ識別情報を第1装置が受信するステップ、および第1装置から送信するユーザ識別情報を変更後のユーザ識別情報に更新するステップをさらに含むものである。

【0017】請求項10に記載の無線通信方法は、ユーザが携帯可能でありかつ無線通信可能な第1装置と無線通信可能な第2装置との無線通信方法であって、第1装置からユーザごとの固有のユーザ識別情報を第2装置に送信するステップ、第1装置からのユーザ識別情報を第2装置が受信するステップ、第2装置が受信したユーザ識別情報を変更するステップ、第2装置から第1装置に変更後のユーザ識別情報を送信するステップ、第2装置から送信された変更後のユーザ識別情報を第1装置が受信するステップ、および第1装置から送信するユーザ識別情報を変更後のユーザ識別情報に更新するステップを備える。

【0018】請求項11に記載の無線通信方法は、ユーザ識別情報はユーザIDとパスワードとを含み、かつ第2装置はユーザIDとパスワードとに基づいてファイルが管理可能に構成されるときに用いられる無線通信方法であって、請求項9または10に記載の無線通信方法において、第1装置からのユーザIDに基づいて特定されるファイルのパスワードを更新するステップをさらに含むものである。

【0019】請求項12に記載の無線通信方法は、請求項8ないし11のいずれかに記載の無線通信方法において、第1装置からユーザ識別情報が周期的に送信されるものである。

【0020】請求項13に記載のコンピュータ読み取り可能な記録媒体は、ユーザが携帯可能でありかつ無線通信可能な第1装置と無線通信可能な第2装置との無線通信を行うためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、第1装置からユーザごとの固有のユーザ識別情報を第2装置に送信させる処理、第1装置からのユーザ識別情報を第2装置に受信させる処理、第2装置が受信したユーザ識別情報に基づいてユーザを識別させる処理、およびユーザ識別結果に従ってユーザに利用許可を与えさせる処理をコンピュータに実行させるためのプログラムを記録したものである。

【0021】請求項14に記載のコンピュータ読み取り可能な記録媒体は、請求項13に記載のコンピュータ読み取り可能な記録媒体において、第2装置が受信したユーザ識別情報を変更させる処理、第2装置から第1装置

に変更後のユーザ識別情報を送信させる処理、第2装置から送信された変更後のユーザ識別情報を第1装置に受信させる処理、および第1装置から送信するユーザ識別情報を変更後のユーザ識別情報に更新させる処理をコンピュータに実行させるためのプログラムをさらに記録したものである。

【0022】請求項15に記載のコンピュータ読み取り可能な記録媒体は、ユーザが携帯可能でありかつ無線通信可能な第1装置と無線通信可能な第2装置との無線通信を行うためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、第1装置からユーザごとの固有のユーザ識別情報を第2装置に送信させる処理、第1装置からのユーザ識別情報を第2装置に受信させる処理、第2装置が受信したユーザ識別情報を変更させる処理、第2装置から第1装置に変更後のユーザ識別情報を送信させる処理、第2装置から送信された変更後のユーザ識別情報を第1装置に受信させる処理、および第1装置から送信するユーザ識別情報を変更後のユーザ識別情報に更新させる処理をコンピュータに実行させるためのプログラムを記録したものである。

【0023】請求項16に記載のコンピュータ読み取り可能な記録媒体は、ユーザ識別情報はユーザIDとパスワードとを含み、かつ第2装置はユーザIDとパスワードとに基づいてファイルが管理可能に構成されるときに用いられるコンピュータ読み取り可能な記録媒体であって、請求項14または15に記載のコンピュータ読み取り可能な記録媒体において、第1装置からのユーザIDに基づいて特定されるファイルのパスワードを更新させる処理をコンピュータに実行させるためのプログラムをさらに記録したものである。

【0024】請求項17に記載のコンピュータ読み取り可能な記録媒体は、請求項13ないし16のいずれかに記載のコンピュータ読み取り可能な記録媒体において、第1装置からユーザ識別情報を周期的に送信させる処理をコンピュータに実行させるためのプログラムをさらに記録したものである。

【0025】請求項1に記載の無線通信システムでは、ユーザが携帯している第1装置から送信されたユーザ識別情報を第2装置が受信すると、第2装置では、そのユーザ識別情報に基づいてユーザが識別され、利用権を有するユーザか否かが判断される。判断の結果、利用権を有するユーザであればそのユーザに利用許可が与えられるが、利用権を有さないユーザには利用が許可されない。

【0026】このように、ユーザは、ユーザ識別情報を自ら入力することなく自動的に利用許可が与えられるか否かが判断され、煩雑な操作が不要となる。また、利用を許可されているユーザが第2装置から離れその間に他人が第2装置を利用しようとしても、他人には利用許可は与えず、ユーザ情報の秘匿性を十分に保護できる。

【0027】請求項2に記載の無線通信システムでは、第2装置によって自動的に変更されたユーザ識別情報が第1装置に送信され、第1装置から送信されるユーザ識別情報が更新される。したがって、ユーザが定期的にユーザ識別情報を変更する煩わしさを回避でき、しかもユーザ識別情報の解読が困難になり、セキュリティをより向上できる。

【0028】請求項3に記載の無線通信システムでは、請求項1に記載の無線通信システムと同様、煩雑な操作を行うことなく他人の利用を阻止できるだけでなく、請求項2と同様、自動的にユーザ識別情報を更新できるので、ユーザがユーザ識別情報を変更する煩わしさを回避でき、しかもユーザ識別情報の解読が困難になり、セキュリティをより高めることができる。

【0029】請求項4に記載の無線通信システムでは、さらに、第1装置から送信されるユーザIDに基づいて特定されたファイルのパスワードが、送信されたパスワードに更新される。したがって、第2装置が管理する個々のファイルをユーザIDとパスワードとに基づいて管理できるだけでなく、ファイル毎のパスワードが自動的に更新されるので、各ファイルのパスワードの解読が困難になり、セキュリティを高めることができる。

【0030】また、請求項5に記載するように、第1装置からユーザ識別情報を周期的に送信すれば、それに応じて第2装置では周期的にユーザ識別が行われる。

【0031】請求項6に記載するように、第1装置と第2装置とを赤外線によって通信すれば、簡単な構造で無線通信システムを構築することができる。

【0032】請求項7に記載するように、たとえば第1装置に携帯機器を、第2装置にパソコンを用いれば、パソコンを利用可能なユーザ識別情報が格納された携帯機器を所持しているユーザだけがパソコンを利用することができる。

【0033】なお、請求項8～12に記載の無線通信方法においても同様である。また、請求項13～17に記載のコンピュータ読み取り可能な記録媒体に格納されているプログラムを用いて無線通信システムを動作させるときも同様である。

【0034】

【発明の実施の形態】以下、この発明の実施の形態について図面を参照して説明する。

【0035】図1および図2を参照して、この実施の形態の無線通信システム10は、それぞれたとえば赤外線によって通信可能な携帯機器10aとパソコン10bとを含む。

【0036】携帯機器10aはたとえばユーザの衣服などに装着可能なバッジのような装置で構成される。携帯機器10aは、携帯機器10aの動作制御を行うためのプログラム、図7～図11の各(a)に示す処理を実行するためのプログラムやデータが格納されるROM1

2、ユーザ毎の固有のユーザ識別情報、フレームデータなどが格納されるRAM14、赤外線通信中の時間管理をするタイマ16、赤外線を発光または受光する赤外線受発光素子18、赤外線受発光素子18を制御する赤外線制御部20、およびこれらを制御するためのCPU22を含む。

【0037】一方、パソコン10bは、パソコン10bの動作制御を行うためのプログラム、図7～図11の各(b)に示す処理を実行するためのプログラムやデータが格納されるハードディスク24、パソコン10bの利用権を有するユーザの識別情報、フレームデータなどが格納されるRAM26、CD-ROM(図示せず)内の情報を読み出すためのCD-ROMドライブ28、フロッピーディスク(図示せず)に情報を読み書きするためのフロッピーディスクドライブ30、インターネット等に接続するためのネットワーク接続装置32、赤外線を発光または受光するための赤外線受発光素子34、赤外線受発光素子34を制御する赤外線制御部36、赤外線通信中の時間管理をするタイマ38、これらを制御するためのCPU40を含む。

【0038】なお、図7～図11の各(b)に示す処理を実行するためのプログラムやデータは、ハードディスク24に予め格納される他、CD-ROMやフロッピーディスクに格納されている場合にはそれぞれCD-ROMドライブ28やフロッピーディスクドライブ30を介してパソコン10bで利用することができ、さらには、インターネット等を通じてダウンロードすることによってパソコン10bで利用することができる。また、ROM12、ハードディスク24、CD-ROM、フロッピーディスク等のそれぞれの記録媒体には、携帯機器10a用のプログラムとパソコン10b用のプログラムとを区別することなく、図7～図11の処理を実行するためのプログラムが格納されてもよいことはいうまでもない。

【0039】このような携帯機器10aからパソコン10bへは、ユーザ識別情報を含むデータが赤外線通信によってフレーム単位で、たとえば図3に示すように周期的(ここでは時間間隔T1毎)に送信される。

【0040】フレームは、たとえば図4に示すように構成され、フレームの開始を示すBOF(Beginning of Frame)、フレームの終結を示すEOF(End of Frame)、通信相手を示すアドレスが格納されるアドレス部、フレームの種別を示す制御部、ユーザIDやパスワードなどを含むユーザ識別情報、伝送エラー検出のためのビット列であるCRCを含む。

【0041】また、パソコン10bのハードディスク24に格納されるファイルは、たとえば図5に示すように構成され、ファイル名、ファイルのサイズ、ファイルの種類、ファイルの更新日時、ファイルのユーザID、ファイルのユーザのパスワードを含む。

【0042】ここでユーザIDおよびパスワードは、たとえば図6に示すように、それぞれ「Tanaka」および「kfo87b」などによって構成される。

【0043】このように構成される無線通信装置10の動作について説明する。

【0044】図7(a)に示すように、まず、携帯機器10aからは、ユーザ識別情報を含むフレームがパソコン10bに送信され(ステップS1a)、タイマ16において時間Tがゼロにリセットされ(ステップS3a)、タイマ16の計時がスタートされる(ステップS5a)。そして、タイマ16によって計時される時間Tが時間間隔T1より大きい($T > T1$)か否かが判断され(ステップS7a)、 $T > T1$ になるまで待機する。 $T > T1$ になれば、ステップS1に戻り、ユーザ識別情報が送信される。このようにして携帯機器10aからは周期的(時間間隔T1毎)にユーザ識別情報がパソコン10bに送信される。

【0045】一方、図7(b)に示すように、パソコン10bでは、まず、タイマ38において時間Tがゼロにリセットされ(ステップS1b)、タイマ38の計時がスタートされる(ステップS3b)。そして、携帯機器10aからのユーザ識別情報が受信されたか否かが判断され(ステップS5b)、受信するまで待機し、ユーザ識別情報が受信されると、タイマ38によって計時される時間Tが任意に設定された時間間隔T2より大きい($T > T2$)か否かが判断される(ステップS7b)。 $T > T2$ でなければ、受信されたユーザ識別情報が、RAM26に登録されている識別情報と一致するか否かが判断され(ステップS9b)、一致すればそのユーザにパソコン10bの利用が許可され、ステップS1bに戻る。

【0046】一方、ステップS7bにおいて $T > T2$ のとき、またはステップS9bにおいて、受信されたユーザ識別情報が登録されている識別情報と一致しなければ、そのユーザにはパソコン10bの利用が許可されず(ステップS13b)、ステップS1bに戻る。

【0047】したがって、識別処理の結果パソコン10bの利用権を有するユーザに対してのみパソコン10bの利用が許可される。

【0048】このように動作させることによって、パソコン10bの利用権を有するユーザは、ユーザ識別情報を入力するという煩雑な操作を行うことなく、自動的にユーザ識別処理によって利用許可が与えられ、ユーザにとって簡易でかつ有効なユーザ識別機能を有する無線通信システム10が得られる。

【0049】また、携帯機器10aからパソコン10bへ周期的にユーザ識別情報を送信し、周期的にユーザ識別が行われるので、たとえば利用を許可されているユーザがパソコン10bから離れ所定時間以上(ここでは、 $T > T2$ となるまで)戻らなければ、パソコン10bは

利用することができなくなる。したがって、たとえば、利用が許可されているユーザがパソコン10bから離れている間に他人がそのパソコン10bを利用しようとしても許可されず、ユーザ情報の秘匿性を十分に保護できる。この場合、利用権を有するユーザが再びパソコン10bを操作するときには、そのユーザがパソコン10bと向かい合うだけで、ユーザ識別処理が行われ、その結果再びパソコン10bは利用可能となる。特に、この発明は、1台のパソコンを複数人が使用する場合のセキュリティに有効となる。

【0050】なお、携帯機器10aからパソコン10bへユーザ識別情報を送信する周期が短いほど、ユーザ識別処理をきめ細かく行えることは容易に理解されよう。

【0051】また、図8に示すように、ユーザ識別情報を自動的に更新することもできる。ここでは、ユーザ識別情報に含まれるユーザIDとパスワードとのうち、変更される（新たに生成される）のはパスワードだけであり、ユーザIDは変更されない場合を想定して説明を進める。以下に述べる他の動作例についても同様である。

【0052】この場合、図8(a)に示すように、まず、携帯機器10aからは、ユーザ識別情報を含むフレームがパソコン10bに送信され（ステップS21a）、タイマ16において時間Tがゼロにリセットされ（ステップS23a）、タイマ16の計時がスタートされる（ステップS25a）。そして、パソコン10bからの新しいユーザ識別情報が受信されたか否かが判断される（ステップS27a）。新しいユーザ識別情報が受信されなければ、タイマ16によって計時される時間Tが時間間隔T2より大きい（ $T > T2$ ）か否かが判断され（ステップS29a）、 $T > T2$ でなければステップS27aに戻る。T>T2になれば終了する。

【0053】ステップS27aにおいて、新しいユーザ識別情報が受信されると、それまでのユーザ識別情報が新しいユーザ識別情報に更新され、RAM14に記憶され（ステップS31a）、ステップS21aに戻り、その後は、新しいユーザ識別情報がパソコン10bに送信される。

【0054】一方、図8(b)に示すように、パソコン10bでは、まず、タイマ38において時間Tがゼロにリセットされ（ステップS21b）、タイマ38の計時がスタートされる（ステップS23b）。そして、携帯機器10aからのユーザ識別情報が受信されたか否かが判断され（ステップS25b）、受信するまで待機し、ユーザ識別情報が受信されると、タイマ38によって計時される時間Tが時間間隔T2より大きい（ $T > T2$ ）か否かが判断される（ステップS27b）。T>T2でなければ、たとえば乱数処理によって新しいユーザ識別情報が生成され（ステップS29b）、その新しいユーザ識別情報が携帯機器10aに送信され（ステップS31b）、ステップS21bに戻る。ステップS27bに

において $T > T2$ のときには終了する。

【0055】このようにT>T2を満たすまで、携帯機器10aからパソコン10bへ周期的にユーザ識別情報が送信され、それに応じてパソコン10bにおいてユーザ識別情報が周期的かつ自動的に変更され、変更されたユーザ識別情報が携帯機器10aとパソコン10bとの間で送受信される。したがって、ユーザ識別情報の解読が困難になり、セキュリティをより高めることができる。

10 【0056】なお、ステップS29bにおける新しいユーザ識別情報の生成は、携帯機器10aからユーザ識別情報が送信される毎に行われるが、それに限定されず、たとえば定期的に行われてもよい。

【0057】さらに、図9に示すように、ユーザ識別情報を自動的に更新しかつユーザを識別することもできる。

【0058】この場合、図9(a)のステップS41a～S51aに示す携帯機器10aの動作は、図8(a)のステップS21a～S31aと同様であるので、その重複する説明は省略する。ただし、図8(a)とは異なり、図9(a)では、ステップS49aにおいて $T > T2$ であればステップS41aに戻る。

20 【0059】一方、図9(b)のステップS41b～S53bに示すパソコン10bの動作は、図7(a)のステップS1b～S13bと同様であるので、重複する説明は省略する。なお、図9(b)ではさらに、ステップS51bの後、たとえば乱数処理によって新しいユーザ識別情報が生成され、RAM26に登録されている識別情報が新しいユーザ識別情報に更新され（ステップS55b）、その新しいユーザ識別情報が携帯機器10aに送信され（ステップS57b）、ステップS41bに戻る。

【0060】このような一連の処理が周期的に繰り返され、パソコン10bの電源を切るまで続けられる。ユーザの携帯機器10aには、最終的にパソコン10bの電源を切る直前に送信されたユーザ識別情報が記憶される。次回ユーザがパソコン10bを起動させたときには、携帯機器10aに記憶されたユーザ識別情報が送信され、パソコン10bでユーザ識別処理が行われる。利用可能なユーザとして識別されれば、一連のユーザ識別情報の送受信が行われる。

【0061】このように、煩雑な操作なしに自動的に生成されるユーザ識別情報に基づいてユーザ認識処理が可能になる。また、自動的にユーザ識別情報を更新できるので、ユーザ識別情報を変更する煩雑さを回避できかつセキュリティを向上できる。したがって、信頼性が高くかつ簡易にユーザを識別することができる無線通信システム10が得られる。

【0062】さらに、図10に示すように、ユーザ識別情報を携帯機器10aからパソコン10bに送信する際

に、パソコン 10b で作成したファイルの属性にユーザ識別情報を反映させることによって、個人毎の効果的なファイル管理を実現することができる。

【0063】この場合、図 10 (a) のステップ S61a ~ S71a に示す携帯機器 10a の動作は、図 8 (a) のステップ S21a ~ S31a と同様であるので、その重複する説明は省略する。

【0064】一方、図 10 (b) のステップ S61b ~ S69b に示すパソコン 10b の動作は、図 8 (a) のステップ S21b ~ S29b と同様であるので、重複する説明は省略する。なお、図 10 (b) ではさらに、ステップ S69b によって新しいユーザ識別情報が生成された後、携帯機器 10a から受信したユーザ ID と同じユーザ ID を有するファイルのパスワードが、新しいパスワードに更新され、RAM26 に記憶される (ステップ S71b)。そして、新しいユーザ識別情報が携帯機器 10a に送信され (ステップ S73b)、ステップ S61b に戻る。

【0065】 $T > T2$ を満たすまで、携帯機器 10a からパソコン 10b へ周期的にユーザ識別情報が送信され、それに応じてパソコン 10b においてパスワードが周期的かつ自動的に変更され、変更されたパスワードを含むユーザ識別情報が携帯機器 10a とパソコン 10b との間で送受信される。そして、パソコン 10b に保存されているファイルのうち、受信したユーザ ID と同じユーザ ID を有するファイルのパスワードが、新しく生成されたパスワードに更新され、ファイルが保存される。

【0066】このように動作させることによって、各ファイルのパスワードの解読が困難になり、パソコン 10b および各ファイルのセキュリティをより高めることができる。

【0067】また、図 11 に示すように、パソコン 10b で作成したファイルの属性にユーザ識別情報を反映させることによって、個人毎の効果的なファイル管理を実現し、さらに、ファイルのパスワードを自動的に更新し、かつユーザを識別することもできる。

【0068】この場合、図 11 (a) のステップ S81a ~ S91a に示す携帯機器 10a の動作は、図 8 (a) のステップ S21a ~ S31a と同様であるので、その重複する説明は省略する。ただし、図 8 (a) とは異なり、図 11 (a) では、ステップ S89a において $T > T2$ であればステップ S81a に戻る。

【0069】一方、図 11 (b) のステップ S81b ~ S93b に示すパソコン 10b の動作は、図 7 (a) のステップ S1b ~ S13b と同様であるので、重複する説明は省略する。なお、図 11 (b) ではさらに、ステップ S91b においてユーザにパスワード 10b の利用を許可した後、たとえば乱数処理によって新しいユーザ識別情報が生成され、RAM26 に登録されている識別

情報が新しいユーザ識別情報に更新され (ステップ S95)、その後、携帯機器 10a から受信したユーザ ID と同じユーザ ID を有するファイルのパスワードが、新しいパスワードに更新され、RAM26 に記憶される (ステップ S97b)。そして、新しいユーザ識別情報が携帯機器 10a に送信され (ステップ S99b)、ステップ S81b に戻る。

【0070】このような一連の処理が周期的に繰り返され、パソコン 10b の電源を切るまで続けられる。

【0071】このように動作させることによって、煩雑な操作なしに自動的に生成されるユーザ識別情報に基づいてユーザ認識処理が可能になる。また、自動的にユーザ識別情報を更新できるので、ユーザ識別情報を変更する煩雑さを回避できかつセキュリティを向上できる。さらに、ユーザ ID およびパスワードのユーザ識別情報を利用してユーザ識別を自動的に行い、ファイル管理することによって、信頼性が高く、簡易かつ効率的なファイル管理を実現できる。また、ファイルのパスワードを自動的に更新できるので、各ファイルのセキュリティを向上できる。

【0072】なお、この発明は、赤外線通信可能な装置に限定されず、他の任意の無線によって通信可能な装置に適用できる。

【0073】また、携帯機器 10a としては、PDA (Personal Digital Assistants) が用いられてもよく、パソコン 10b の代わりにワークステーション等が用いられてもよい。

【0074】さらに、上述の実施の形態では、ユーザ識別情報はユーザ ID とパスワードとを有する場合について述べたが、ユーザ識別情報はパスワードだけで構成されてもよい。

【0075】

【発明の効果】この発明によれば、煩雑な操作を行うことなく利用権を有するユーザとそれ以外のユーザとを識別でき、ユーザ情報の秘匿権保護を効果的に実現できる。

【図面の簡単な説明】

【図 1】この発明の一実施形態の無線通信システムを示す概略図である。

【図 2】この発明の一実施形態を示すブロック図である。

【図 3】ユーザ識別情報を送受信する時間間隔を示す図解図である。

【図 4】フレームフォーマットの一例を示す図解図である。

【図 5】ファイルフォーマットの一例を示す図解図である。

【図 6】ユーザ ID およびパスワードの一例を示す図解図である。

【図 7】この発明の第 1 の動作例を示すフロー図であ

り、(a)は携帯機器の動作、(b)はパソコンの動作を示す。

【図8】この発明の第2の動作例を示すフロー図であり、(a)は携帯機器の動作、(b)はパソコンの動作を示す。

【図9】この発明の第3の動作例を示すフロー図であり、(a)は携帯機器の動作、(b)はパソコンの動作を示す。

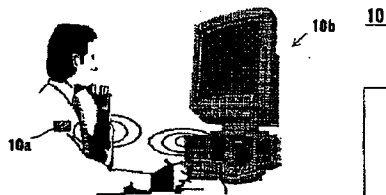
【図10】この発明の第4の動作例を示すフロー図であり、(a)は携帯機器の動作、(b)はパソコンの動作を示す。

【図11】この発明の第5の動作例を示すフロー図であり、(a)は携帯機器の動作、(b)はパソコンの動作を示す。

【符号の説明】

- 10 無線通信システム
- 10a 携帯機器
- 10b パソコン
- 12 ROM
- 14、26 RAM
- 16、38 タイマ
- 18、34 赤外線受発光素子
- 20、36 赤外線制御部
- 22、40 CPU
- 24 ハードディスク
- 28 CD-ROMドライブ
- 30 フロッピーディスクドライブ
- 32 ネットワーク接続装置

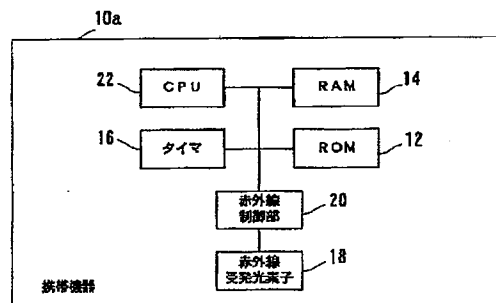
【図1】



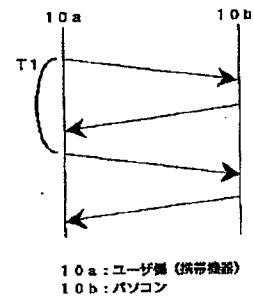
【図6】

ユーザID : Tanaka
パスワード : kfo87b

【図2】



【図3】



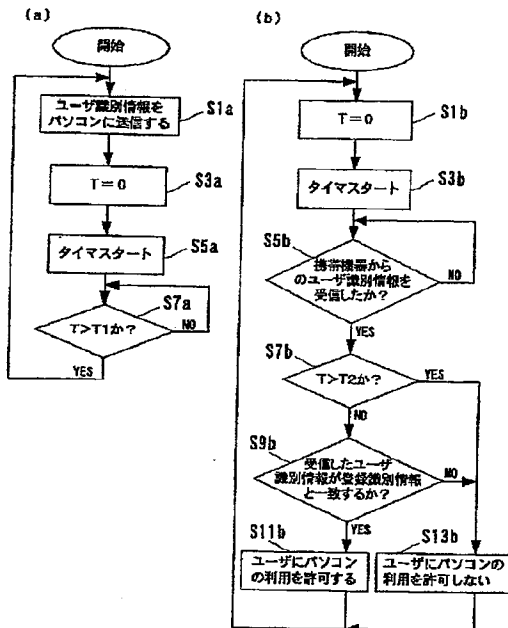
【図4】

BOF	アドレス部	制御部	ユーザ識別情報	CRC	EOF
-----	-------	-----	---------	-----	-----

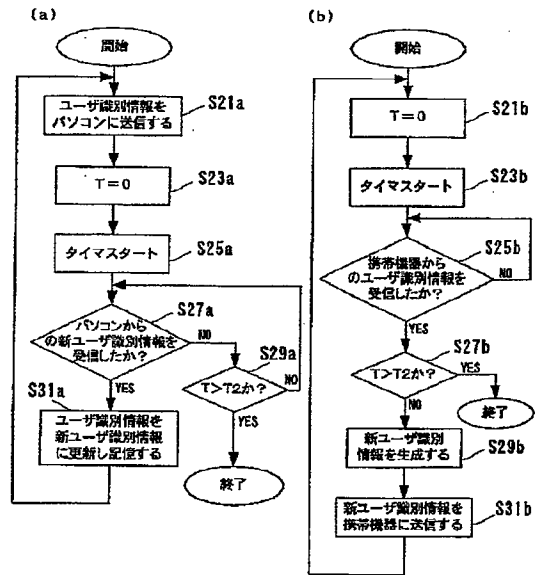
【図5】

ファイル名	サイズ	ファイルの種類	更新日時	ファイルのユーザID	ファイルのユーザのパスワード
-------	-----	---------	------	------------	----------------

【図7】

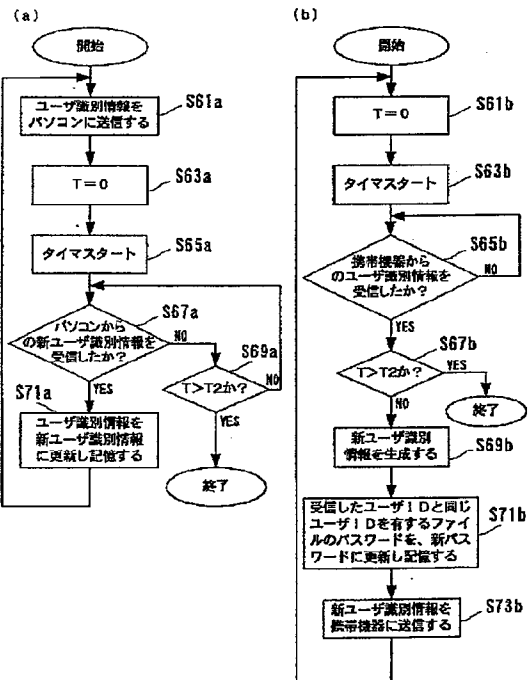
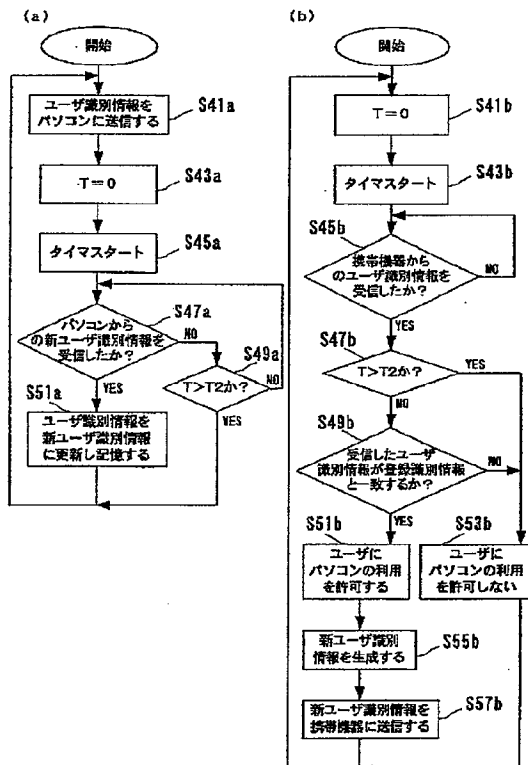


【図8】

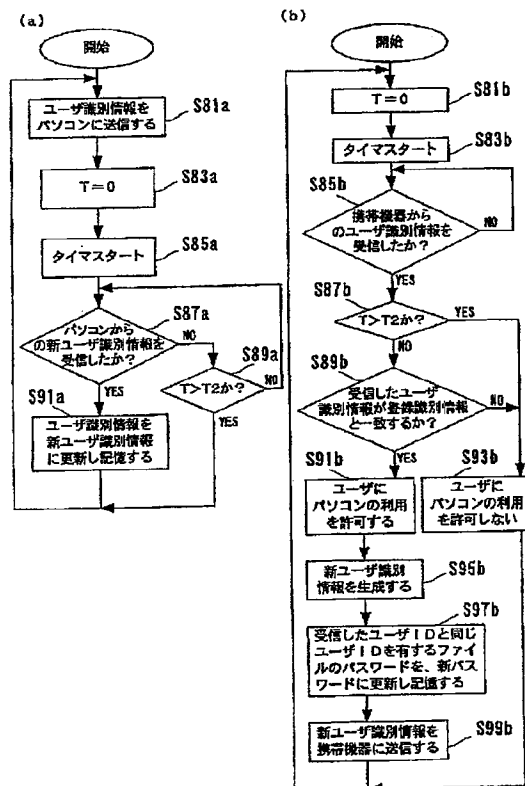


【図10】

【図9】



【図11】



フロントページの続き

Fターム(参考) 5J104 AA07 KA01 NA05 NA27 PA01
 PA07
 5K067 AA33 AA34 BB21 DD17 EE02
 HH22 HH23